HOLDOVER
"The basic publication has changed; impact on supplemental information is under review by the OPR. Users should follow supplemental information that remains unaffected."

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the HQ AFMC WWW site at: https://www.afmc-mil.wpafb.af.mil/pdl/.

This supplement applies to all Air Force military and civilian personnel, including Air National Guard or US Air Force Reserve (AFRES) and their use of public internet and web technology such as web servers, web browsers, and file transfer protocol (FTP) software purchased and licensed by the United States Air Force (USAF), or privately licensed software used with proper approval on USAF-owned systems. Units may further supplement this Air Force Instruction and Command Supplement, as required. Field units will send their drafts and copies of their supplements to HQ AFMC/SCPI, Bldg 266, Rm A112, 4225 Logistics Avenue, Wright-Patterson AFB OH 45433-5744.

SUMMARY OF REVISIONS

This revision added several new areas such as new policy regarding World Wide Web (WWW) server administration and support, indexing, WWW page organization and maintenance, and information review and release. It also adds responsibility for recurring training for OPRs and Page Maintainers to the Communications Systems Security Officers' (CSSO) initial and annual training requirement. Roles of the Multi-Disciplinary Review Board have been further expanded and defined. A checklist for OPRs and Page Maintainers for use before posting information to the internet has been added. Plans and procedures to establish, maintain & review web sites, and the HQ USAF "warning banner" for public and restricted web pages have been added. This revision updates information regarding local-level internet use, internet use by chartered organizations, updates guidance on contractor-developed and maintained systems con-

taining government information, and adds a command-level web site recognition program. Information Assurance (IA) procedures have been updated in this supplement.

AFI 33-129, 1 August 1999, is supplemented as follows:

3.3.1. Reviews will be conducted annually on 1 Oct of the given year. The board may also convene as necessary at the discretion of the installation Designated Approval Authority (DAA) to address local internet issues as required. The findings of the review boards will be sent to HQ AFMC/SCPI along with the date action will be complete. Review boards will be chaired by the installation DAA and should consist of representatives from communications & information, public affairs, legal, contracting, operations, and other functional area experts at the installation level along with members of the installation web administration team.

3.4.1. AFMC field units will follow the plans provided within this supplement.

3.4.2. This function will be part of the annual inspection by the review board.

3.4.5. All web sites must be reviewed by the base PA office prior to their launch.

All web pages will follow and apply the guidance adhered to in Air Force Communications Agency homepage development at the following URL: **https://www.afca.scott.af.mil/eim/webstylehome.htm**.

3.6.1. Do not use the web to advertise private or unofficial organization fundraising activities (DOD 5500.7-R, *Joint Ethics Regulation (JER)*). This also applies to chartered organizations authorized to establish web pages or sites (see **paragraph 6.4**).

3.6.5. (Added) Approve all information placed on the web by their organization. May delegate approval authority, in writing, no lower than office chief. Ensure content is mission-related, sensitivity of information and associated risk of loss have been considered and security features, such as access control, encryption, etc., are sufficient. Ensure that OPSEC considerations are addressed and critical information for the organization is defined and disseminated. Chartered organizations, when authorized, must have an internet page approved in their charter approved through the local installation (see **paragraph 6.4**).

3.6.6. (Added) Ensure all units and organizations, whether temporary or permanent, that use the base netw.ork comply with this instruction and this supplement.

3.6.7. (Added) Ensure all contractor-developed web sites/pages and information are placed on the official government web servers, and where practical, those located at the Network Control Center (NCC) for centralized control (see **paragraph 10.3 (Added)**).

3.8.5. (Added) Establish two physically separate servers, one for public access and one for ".mil" (restricted) access. Ensure authorized web servers are certified and accredited IAW AFSSI 5024, Vols. I and II, *The Certification and Accreditation (C&A) Process*, and are located in and controlled by the Network Operations and Security Center (NOSC) or the NCC.

3.8.6. (Added) Audit the network continually to locate unauthorized public-access web servers and unapproved restricted-access web servers. For unauthorized public-access web servers, contact the responsible information provider/OPR, move the data to the NOSC/NCC server, and take action to disconnect the unauthorized public-access server from the network. For unapproved restricted-access web servers, notify the responsible information provider/OPR to obtain C&A (see **paragraph 10.1**) and report the incident, along with required actions for protecting the network and information, to the Base Information Assurance Officer (BIAO) and the comm unit commander.

3.9.1. (Added) CSSOs are additionally responsible for, as part of the initial and annual training requirement, ensuring OPRs and page maintainers are educated on their roles and responsibilities. CSSOs will also ensure all users are educated on Air Force, command and local policies regarding official and authorized internet use.

3.10.2. Ensure the information is suitable for transmission on the internet. If the posted information may pose OPSEC or other security concerns, report it to the web page point of contact and the appropriate security personnel for clarification/resolution.

3.10.3. Use AFI 51-303, *Intellectual Property—Patents, Patent-Related Matters, Trademarks and Copyrights*, and AFI 33-360, Vol 1, *Publications Management Program*, for guidance on how to obtain approval to use copyright and trade name information, and how to mark the web page.

3.11.1. Before posting public access information to the web, coordinate the information with the Public Affairs Office. Information includes text, pictures, and graphics.

3.11.4. The information provider/OPR will conduct a monthly review of functional web sites and pages to ensure all links are valid and information is current.

3.14. Multi-Disciplinary Review Board responsibilities also include, but are not limited to, providing customer input, hardware/software requirements, security recommendations, and educating and maintaining the awareness of the world wide web and policies regarding its use within AFMC. The board will also study initiatives and proposals for government contractor developed, maintained, or stored (outside of the ".mil" domain) government programs and software. (Refer to **paragraph 10.3 (added)**).

4.1. This information should be distinguishable from other information on the top page of the web server.

4.1.1.1. (Added) Training for web server administrators:

4.1.1.1.1. (Added) Hypertext Markup Language (HTML). Training requirement for webmasters in order to develop host server's top-level pages and to assist Page Maintainers who will maintain lower level web sites.

4.1.1.1.2. (Added) Graphics Format and Conversion. Quality graphics and presentation are essential in web development. Web server administrators are required to have this training in order to develop host server's top-level pages and to assist Page Maintainers who will maintain lower level web sites.

4.1.1.1.3. (Added) Indexing. Each AFMC web server is required to have a searchable index for its information. This index will be consistent with the information's various access and security controls. It is essential webmasters be proficient in server indexing software and indexing techniques.

4.1.1.1.4. (Added) Quality Performance Indicators (QPIs). Webmasters are required to be proficient in employing tools to provide adequate performance statistics (server usage, page accesses, etc.) for their customers.

4.1.1.1.5. (Added) Recommended Webmaster Requirements. In addition to the core webmaster requirements, it is strongly recommended webmasters have an adequate background in programming/scripting (Perl, etc.), database interfacing, and multimedia authoring. The future of the web and internet will involve interfacing legacy systems with web pages.

4.1.1.2. (Added) Certified Systems Administrator Training. Training requirement for webmasters based on the platform and software used to operate the specific World Wide Web server being administered.

Training is commonly available from the specific platform or software vendor and should include background in system security and other networking functions associated with the server to be administered.

4.2. The number of Page Maintainers should be limited to the minimum needed to service the organization.

4.2.1.3. Page maintainers will conduct a monthly review of each site to determine links are valid and sites conform to style guidance (see **paragraph 3.4.6.**). Information providers/OPRs verify information content and notify page maintainers when to remove or change information (see **paragraph 3.11.4**).

4.2.1.6. Passwords will be changed every 90 days for security reasons.

6.1. Unit commanders and section chiefs have discretion to determine authorized use of computer systems that are of best interest to the government such as government personnel using them to further their professional and military knowledge. Consideration for internet use related to transitions may be given to military/civilian personnel who are separating, retiring, or who are affected by A-76 studies or base closures. Allowance for this access shall conform to the provisions in Section 6, meet the requirements directed in AFI 33-202 and AFI 33-202, AFMC Sup 1, and not interfere with the conduct of official business. Additionally, no additions/downloads of software or modification of government software or equipment for such use is authorized.

6.1.2. Do not use the web to advertise private or unofficial organization fundraising activities (DOD 5500.7-R, **Joint Ethics Regulation (JER)**).

6.1.6. Use of Internet Relay Chat (IRC) for any purpose. Additionally, participation in 'chat lines' or discussion forums (bulletin boards, news groups, etc.) except those that have been approved through Public Affairs channels and reside on restricted-access government web pages.

6.1.13. (Added) Using government-provided software to directly connect to non-government email servers. Such connections create alternative routes for non-monitored email traffic, and therefore pose a direct threat to the base network.

6.1.14. (Added) Use of personal digital assistants (PDAs) will only be used as authorized in AFI 33-202 paragraph 3.5.3.

6.3.1. (Added) Remote access to base network services shall be accomplished by accessing an account via an NCC-controlled remote access server (RAS) with appropriate encryption (SSL). Account users may be allowed access to e-mail, restricted-access web servers, or even general internet connectivity. RAS configuration/access restrictions will comply with higher headquarters guidance (AFI 33-202, AFSSI 5027, etc.).

6.3.2. (Added) Dial-up internet services accessed from government computer systems must be air-gapped (stand alone) from the base network. These services must be coordinated and approved prior to establishing the connection. The unit commander authorizes submission of the request for evaluation by the BIAO. All requests for organizational ISP subscriptions shall provide assurance that the system does not have base network connectivity and utilizes the latest in anti-virus software in "auto protect" mode. The BIAO, along with CNCC personnel, shall evaluate the risk of the connection as well as determine if the service can be provided via the base network vise an ISP link.

6.4. Where approved by the installation commander and authorized by the Web Server Administrator, non-governmental organizations chartered for the purpose of enhancing morale or providing mission support to military installations or units (e.g., Top-3, Booster Clubs, Advisory Councils, Chiefs' Groups, First

Sergeants' Councils, Company Grade Officers' Associations) may maintain an informational web page on government internet servers. The organization's charter must specifically authorize the organization to maintain a web page, and the organization must obtain approval from the base legal office (JA). By default, any web page developed under the authority of this paragraph will be treated as "official" and will be located on the installation's restricted-access web servers. With Public Affairs clearance and approval through directed channels (See Section 7), the information/web pages may be placed on public-access web servers. In addition, the web page will not cause undue strain on equipment, software, network servers or system resources. Web pages must follow the guidelines set forth in **paragraph 6.1.2** above. Web pages are to be informational only; they may not be used to advertise products, solicit funds, or for any other commercial purposes. Violation of these prohibitions will result in immediate removal of the offending page from the server.

6.4.1. (Added) HQ AFMC/SC is the approving authority of dial-up internet service for foreign nationals (including Foreign Liaison Officers). The ISP or RAS access will be IAW AFI 33-202, AFMC Sup 1, and AFMC/CV Policy message, *Interim Policy for Foreign National Access to AFMC Unclassified Computer Systems and Information*, 161500Z Jun 00.

7.1. Information Providers/OPRs for web sites and pages are responsible for obtaining necessary coordination and approval and for keeping the information current.

7.2. Prior to posting public access information to the web, coordinate the information with the Public Affairs Office. Information includes text, pictures, and graphics.

7.2.1.2. The local Public Affairs Office coordinates on all web page information (text, pictures, graphics, sound, and video). Any information deemed not appropriate for public release will be limited to restricted-access servers.

7.2.1.3. (Added) 5 USC 552(a)(2)(D), Electronic FOIA (EFOIA), and DoD 5400.7/Air Force Supplement require records that an agency determines likely to be the subject of subsequent or frequent FOIA requests be placed in a FOIA Reading Room on public-access servers. The local FOIA Office will manage these reading rooms and link the site to the Air Force FOIA web site (http://www.foia.af.mil). The FOIA Officer, in coordination with the functional OPR/owner of the records, will determine whether the records qualify for posting to the FOIA Reading Room.

7.4.9. (Added) National Security Information. This is sensitive information as defined in Section 3 of Public Law 100-235, *The Computer Security Act of 1987*, maintained in national security systems as defined in Section 2315 of Title 10, United States Code. National Security Information cannot be transmitted across the non-secure internet unless it uses encryption technology approved by the National Security Agency (NSA). (**Note:** As of this writing, no such encryption technology has yet been approved by NSA.) National security information is information which:

7.4.9.1. (Added) Involves intelligence activities.

7.4.9.2. (Added) Involves cryptologic activities related to national security.

7.4.9.3. (Added) Involves the command and control of military forces.

7.4.9.4. (Added) Involves equipment that is an integral part of a weapon or weapons system; or

7.4.9.5. (Added) Is critical to the direct fulfillment of military or intelligence missions--this does not include procurement of automatic data processing equipment or services to be used for routine adminis-

trative and business applications (including payroll, finance, logistics, and personnel management applications).

7.4.9.6. (Added) Information which does not qualify as national security information (for example, some types of Privacy Act and FOUO information) must be encrypted using an encryption technology approved by the National Institute of Standards and Technology (NIST), and comply with Federal Information Processing Standard (FIPS) 140-1. A list of approved encryption technologies is available from NIST. At the time of this writing, the list was available on the web at **http://csrc.ncsl.nist.gov/cryptval/ 140-1/1401val.htm**.

7.5. Commanders will develop a security conscious web posting process tailored to the needs/requirements of their organizations. Such a process shall provide a clear, streamlined method for approving the release of information to the internet.

7.5.1. Locally developed release packages are subject to review during records management staff assistance visits, audits, Information Protection/Information Assurance office assessments, and Inspector General assessments and inspections. If serious violations of policy occur or if information is improperly released, some of the actions the DAA/CSO is authorized to take include removing the non-compliant pages, and disconnecting or shutting down the system in question.

8.1.1. To promote the security and integrity of network systems and information, do not partition a server to separate public from restricted-access information; instead use separate servers. (See **paragraph 3.8.5 (Added)**).

8.1.2. Both official and unofficial bulletin boards are authorized on limited access pages. Information placed on official bulletin boards may include, but not limited to: retirement and promotion ceremonies, commander's call, dining ins/outs. Information placed on unofficial bulletin boards may include, but not limited to: job offers, bake sales, pets & cars for sale, room for rent, yet nothing offensive.

8.2.1.1.10. (Added) There shall be no links from public-access web sites/pages to restricted-access web sites/pages.

8.2.3. Web posting of government e-mail address/telephone number directories is only allowed on restricted pages.

8.2.5. The use of graphics and artwork must be of good taste. Graphics will not be tracked from the information provided or distort the purpose of the web page. Reference Air Force Communication Agencies' site in paragraph 3.4.6 of the supplement.

10.1. Any unauthorized or non-accredited system discovered will be immediately disconnected until the system has been accredited and authorized for use by the DAA. DAAs are appointed in accordance with AFI 33-202_AFMCS1, paragraph 3.2.4 (Added). Tenants will follow the guidance of the host command.

10.3. (Added) Contractor-provided Web Server Support. Web servers hosting official government information must reside on a government-owned, government-controlled network. Official web sites and bulletin boards maintained on a contractor's site, using the contractor's network and resources are prohibited. Organizations may, however, commission contractor support on government furnished equipment at a government site. Contractors providing such support are still subject to all provisions within this instruction. (**Note:** This provision is maintained due to information protection requirements; sharing of information between commercial ".com" or non-government (.edu, .org, etc.) domains and military ".mi/gov" domains may conflict regarding system accreditation standards, government information release guidelines, and other possible information threats.)

10.3.1. (Added) In special cases where resources are not available or location is not accessible (i.e., specialized software, applications, information sharing requirements, dispersed duty locations), a waiver may be requested. The waiver will be coordinated through the following:

10.3.1.1. (Added) Local BIAO, communications squadron commander, and installation commander (including PA/JA coordination to review type of information handled by contractors and potential for public release). The installation DAA and/or multi-disciplinary review board will review such waiver requests and make their recommendations as required. For specific questions on software use, refer to AFI 33-114.

10.3.1.2. (Added) Forward to HQ AFMC/SCP and the command DAA (HQ AFMC/SC) for approval of government information that is contractor stored or maintained at a commercial (.com) or non-military (i.e., .edu, .org, etc. site.) In order to request a waiver, a contract or support agreement must exist, or be in the process of negotiation, with a commercial contractor. The waiver request will contain the following:

10.3.1.2.1. (Added) Exact scope of contract support and purpose supporting the Air Force mission.

10.3.1.2.2. (Added) Why Air Force, DoD, or government resources cannot be utilized.

10.3.1.2.3. (Added) Copies of the support agreement, contract and/or accreditation report of the commercial or contract system (to include information protection requirements to guard against unauthorized release of government information, if the potential exists).

10.3.1.2.4. (Added) Specify how information will be created, maintained, stored, and transferred. Specifically outline information assurance provisions. Must state whether official government records will be generated, and maintained (hardcopy or electronic). (**Note:** Upon termination of support agreement or contract, all software, code, media, and government equipment must be handed over to the government.) Information in AFI 33-129, paragraph 7.4, will not be released to the public.

10.3.2. (Added) Any contractor or agency creating, maintaining, storing, or working with government information in any capacity will have the appropriate security clearance necessary for handling such information. This stipulation should be written into any contract or support agreement.

10.3.3. (Added) Any existing system or software support maintaining official information that is maintained or developed by a contractor or non-government domain and not under Air Force control also requires a waiver in the interests of information assurance and protection.

10.3.4. (Added) Organizations commissioning contractors or non-government agencies will ensure that contractors or non-government agencies utilize government resources at government sites unless a waiver is granted under the criteria above. Again, in unique circumstances where government resources or sites cannot be used, a waiver is required. Such contract support is subject to all provisions of AFI 33-129 and this supplement.

10.3.5. (Added) Waivers must be submitted to HQ AFMC/SC, 4225 Logistics Avenue, Wright Patterson AFB, OH 45433-5744.

11.1.2.4. (Added) Notification of web incident. When a web page has been altered or subject to intrusion, immediately report the incident to the web page maintainer or web master. That person then notifies the CNCC.

Table 1. Line 4. Privacy Act Information. Minimum Access/Security Control- Password and ID/ Encrypted.

Table 1. Note 3 (Added) Transmitting national security information (see paragraph 7.4.9 of this supplement) subject to provisions of Public Law 100-235, *The Computer Security Act of 1987* (as amended), across the non-secure internet is prohibited unless it uses an encryption technology approved by the National Security Agency (NSA). (**Note:** As of this writing, no such encryption technology has yet been approved by NSA.)

12. Data on a web server should be arranged in a hierarchical manner. The server's Home Page should reference the major categories of information maintained within the web server. Try to limit these major categories to no more than seven. The page must include the standard disclaimer/security banner and the name, e-mail, and phone of the webmaster or POC. As a minimum, the following categories are recommended for the web server's Home Page:

Background/Mission. Pointer to mission statement or background information provided by an organization such as Public Affairs or the organization's History Office Organizations or Org Chart. Pointer to page(s) of the organization and next-level subordinate activities.

Search. Pointer to page(s) where full-text ,search and retrieval of information is provided.

What's New. Pointer to page(s) indicating recently added or updated information on the server.

Library. Pointer to area for accessing such things as publications, local and command internet policies, webmaster information, biographies, fact sheets, etc.

Pointers can be added as needed; however, it is imperative web server Home Pages contain only generic pointers to very abstract or "macro-level" subject areas to facilitate the lowest common denominator--the new visitor who knows nothing about the site or the organization. A good benchmark for developing macro-level pointers are "what's inside" sections of newspapers, usually located on the first page. All web pages should be in compliance with Department of Defense Web Site Administration Policies & Procedures, 25 Nov 98, at http://www.defenselink.mil/admin/dod_web_policy_12071998.html   . Guidance and direction for web pages are set forth on the Headquarters Air Force Communications Agency's (HQ AFCA, Scott AFB IL) web site at: **https://www.afca.scott.af.mil/eim/webstylehome.htm**.

13.1. This banner should be placed in a location that's readily visible.

13.2. This banner should be placed in a location that's readily visible.

17. Sensitive But Unclassified (SBU) information must be encrypted during transmission. Public Law 100-235, *The Computer Security Act of 1987* (as amended) establishes the requirement for encryption of national security information. The Act does not distinguish protocols. For example, e-mail's Simple Mail Transfer Protocol (SMTP) is not viewed independently from the web's Hypertext Transfer Protocol (HTTP) or the Internet's File Transfer Protocol (FTP).

18. (Added) Limited Access/Secret Information Protocol Routing Network (SIPRNET). In AFMC, any organization that runs a classified site will review contents for security requirements (i.e., markings, currency of information, access security requirements, etc.). Information providers will immediately remove and/or declassify any information that is no longer relevant to their site or is cleared for downgrading or declassification by the originating classifying authority. New information posted to a classified site may require coordination by the Information Security Office, Foreign Disclosure Office, and Information Provider.

Attachment 3

WEBPAGE PREPARTION CHECKLIST

Section A3A–Checklist for Preparing Material for Public-Release on WWW

A3.1. No list can be all-inclusive in preparing material for the internet, but the following items must be considered. If you cannot answer "yes" to these questions, the material should not be released and should be reworked to fit the criteria, be posted on a limited access site if possible, or not be posted at all.

A3.1.1. Checklist to meet criteria from AFI 33-129, *Transmission of Information via the Internet*:

A3.1.1.1. Is the material of value to the general public? Do not place information that has value to only military or other government agencies on internet pages with unlimited access. (AFI 33-129, *Transmission of Information via the Internet*, paragraph 7.2.1.2).

A3.1.1.2. Is the material free of classified information? (AFI 31-401, *Information Security Program Management*).

A3.1.1.3. Is the material free of Privacy Act-protected information? (AFI 33-332, *Air Force Privacy Act Program*).

A3.1.1.4. Is the material free of For Official Use Only (FOUO) information? FOUO is a marking placed on material to identify contents which are exempt from public release under the Freedom of Information Act (FOIA). Only material which qualifies under FOIA exemptions two through nine can be marked "FOUO." (DoDR 5400.7/AF Sup 1, AFMC Sup 1, *Freedom of Information Act Program*).

A3.1.1.5. Is the material free of FOIA exempt information for which the agency declines to make a discretionary disclosure? To ensure of this, the material should be compared against the nine FOIA exemptions. (DoDR 5400.7/AF Sup 1, AFMC Sup 1).

A3.1.1.6. Is the material free of DoD contractor proprietary information? (AFI 61-204, *Disseminating Scientific and Technical Information (STINFO)*).

A3.1.1.7. Does the material meet the requirements for releasing unclassified STINFO information (free of export-controlled information)? (AFI 61-204).

A3.1.1.8. Is the material free of unclassified information requiring special handling? (AFI 33-113, *Managing Messaging and Data Processing Centers*).

A3.1.1.9. Is the material free of critical information as outlined in AFI 10-1101, *Operations Security (OPSEC) Instructions*? This includes sensitive mission data that by itself is unclassified, but when combined with other available data, may reveal classified information.

A3.1.1.10. Is the material free of phone number and electronic address directories? Publishing such directories is prohibited, because it invites mass mailing by commercial agencies and exposes organizations to attempts to overwhelm local networks. Keep in mind, this does not exclude ALL e-mail and phone numbers; some are required on web pages, and posting general numbers and small blocks of office numbers on lower level pages is encouraged. (AFI 33-129, paragraph 8.2.3., as supplemented).

A3.1.1.11. Is the material free of commercial advertising and product endorsement, and free of graphics and artwork which may be proprietary or copyrighted? (AFI 33-129, paragraphs 8.2.4 and 8.2.5)

A3.1.1.12. Is the material a professional representation of your organization and that of the Air Force?

A3.1.1.13. Is the material timely, current and accurate?

A3.2. If any material meets the following criteria, it may require clearance through the Air Staff or DoD level:

A3.2.1. Is or has the material potential to become an item of national interest or does it have policy implications?

A3.2.2. Does the material concern subjects of potential controversy among DoD components or with other Federal agencies?

A3.2.3. Does the material concern new weapons, weapon systems, or significant modifications or improvement to existing weapons, or systems, equipment, or techniques?

A3.2.4. Does the material concern military operations, operations security, potential operations and significant exercises?

A3.2.5. Does the material concern National Command Authorities and command posts?

A3.2.6. Does the material concern military applications in space, nuclear weapons, including weapon-effects research, chemical warfare, defensive biological and toxin research, high-energy lasers or particle beam technology?

A3.2.7. Does it concern materiel, including that submitted by defense contractors, involving militarily critical technology?

A3.2.8. Does the material concern communications security, signals intelligence and computer security?

A3.3. Primary guidance for releasing information to the public is found in AFI 35-101, *Public Affairs Policies and Procedures*.

Section A3B–Compliance Checklist

A3.4. This compliance checklist is not all-inclusive and should be used as a resource to follow for direction and guidance.

A3.4.1. Are Web pages in compliance with DOD, AF, and HQ AFMC directives?

A3.4.2. Ensure all units and organizations; whether temporary or permanent that use the base enterprise (network) comply with this checklist.

AEnsure a semi-annual review process for each web site to assure yourselves that all links are valid, information is current, and sites conform to the style guidance located at the Headquarters Air Force Communications Agency (HQ AFCA), Scott AFB, IL web site at: **https://www.afca.scott.af.mil/eim/ webstylehome.htm**

A3.4.4. Are Web sites restricted where need be?

A3.4.5. Web Site findings should be documented and reported to appropriate personnel.

A3.4.6. Are Web site restrictions navigated correctly, i.e.

Public sites are public "only" and located on public access only server.

Mil restricted are restricted to ".mil only" server.

A3.4.7. Has accreditation of system been assigned and documented? Web servers should be accredited in accordance with AFSSI 5024, Vols 1 & II, The Certification and Accreditation (C&A) Process.

A3.4.8. Are you informed as to whom your Designated Approval Authority (DAA) is?

A3.4.9. Is privacy act notice included on the main/front page of the web site?

A3.4.10. Are pointers/links up-to-date and operational?

A3.4.11. Is the web page conveying appropriate and current information?

A3.4.12. Ensure procedures are established for management oversight and regular functional review of the Web site.

A3.4.13. Ensure operational integrity and security of the computer and network supporting the Web site are maintained.

A3.4.14. Ensure reasonable efforts are made to verify the accuracy, consistency, appropriateness, and timeless of all information placed on the Web site

A3.4.15. Has all information placed on the Web site been properly reviewed for security, levels of sensitivity and other concerns prior to being released?

Before posting public access information to the web, coordinate the information through fieldPA offices and with HQ AFMC/PA as necessary. Information includes text, pictures, and graphics.

HQ AFMC/PA determines whether the information is pertinent for public release or better suited for restricted access. Information deemed not of public interest or value will be placed on the limited access server.

Follow the local commander's internet release process to ensure proper guidelines for posting information to the web are in place.

A3.4.16. Web sites should not place national security, DOD personnel and assets, mission effectiveness, or the privacy of individuals at an unacceptable level of risk.

A3.4.17. Have HQ AFMC Directors or Chiefs of Staff Offices approved all information placed on the web by their organization?

A3.4.18. Have HQ AFMC Directors or Chiefs of Staff Offices ensured their web's content is mission-related, sensitivity of information and associated risk of loss have been considered and security features, such as access control, encryption, etc., are sufficient?

A3.4.19. Have OPSEC considerations been addressed and critical information for the organization been defined and disseminated?

Attachment 4

PLANS & PROCEDURES TO ESTABLISH, MAINTAIN & REVIEW WEB SITES

A4.1. These Plans and Procedures are not all-inclusive and should be used as a resource to follow for guidance.

A4.1.1. HQ AFMC Directors and Chiefs of Staff Offices have overall authority for web sites within their organization.

A4.1.2. HQ AFMC Directors and Chiefs of Staff Offices may authorize accessing the internet through government computers to further a person's professional growth and military knowledge.

A4.1.3. All Web Pages must support the organization's mission.

A4.1.4. Page Master shall assure the organizations compliance with Department of Defense, Air Force, and HQ AFMC directives.

A4.1.5. All computer users will report any evidence of criminal activity to the command and/or appropriate law enforcement authorities.

A4.1.6. Page Maintainers will manage day-to-day operations.

A4.1.7. Review Board will report (annually) all findings to Page Maintainers.

A4.1.8. Page Maintainers are responsible for the content, navigation, and functionality of their pages.

A4.1.9. Web Masters will take necessary measures to protect Air Force interest in web site usage.

A4.1.10. Consult your organization's information security personnel to ensure that information is suitable for transmission on the internet. If in doubt, contact the unit OPSEC program manager.

A4.1.11. Page Maintainers will take measures to assure all public web pages are approved by field PA offices and HQ AFMC/PA as necessary before they are placed on the internet.

A4.1.12. All web sites with a unique DNS entry, i.e., a base, wing, or MAJCOM must have their web pages registered with the Air Force Link (i.e, http://www.afmc.wpafb.af.mil/). Notice: All of the information between the "//" and the first "/" within the URL. As long as the main page is registered, subordinate sites of the main web page (i.e., http://www.afmc-mil.wpafb.af.mil/organizations/HQ-AFMC/SC/) are also considered registered.

A4.1.13. All web sites must be cleared in accordance with AFI 35-101 and DOD Directive 5230.9, *Clearance of DoD Information for Public Release*.

A All pages should follow and apply the guidance adhered to in Air Force Communications Agency homepage development at the following URL: https://www.afca.scott.af.mil/eim/webstylehome.htm

Appearance

Graphics/imagery should be kept to a minimum.

Graphics should be used only to support the organizations mission.

Non-copyrighted material, text, clip art, hypertext links, images and sound or video clips may be used only if they directly relate to the component's mission.

Web page loads quickly (within 3/5 seconds).

Web page is not cluttered with unnecessary information.

A4.1.15. Air Force members and employees using government communications systems must understand that any type of use, internal, external, authorized or unauthorized, incidental or personal, serves as consent to monitoring.

Attachment 5

AFMC WEB SITE RECOGNITION PROGRAM

A5.1. Purpose. To establish recognition for our outstanding web sites within the command, on a quarterly basis, with emphasis on guidance set forth in AFI 33-129, this supplement, and DoD web policy. This program mirrors, to some degree, the "5-Star" Air Force Public Affairs award program, but differs in that our program will include all sites, both public access and restricted. This program is established with the approval of HQ AFMC/SC.

A5.2. Eligibility & Nomination.

A5.2.1. This program is open to any AFMC unit or staff agency operating a site (home page). Nominations are not restricted to active duty units; the program can also be opened to AFRES/ANG.

A5.2.2. Sites nominated can be either a center/installation site or a group/squadron site with links to subordinate and higher-level echelon units. The particular type of site or function (logistics center, air base wing, or test/acquisition facility) will not be a factor. Sites will be categorized by content (i.e., whether accessible to the public or restricted to "af.mil" access) and scope ((center/wing level), and unit level (group/squadron)). Group level organizations serving as the host on an installation with no Center or Wing assigned will compete at the "Center/Wing" level. Sites will be nominated at the unit's home page level, not an individual section or information page. The communications group or squadron commander, or equivalent will nominate each quarter for AFMC-level recognition, and ensure that any page submitted has been through the required review process (to include PA review if a public access page). This can be delegated to the web-server administrator for command sites. Nominations can be e-mailed or web-entered to HQ AFMC by a predetermined suspense date.

A5.3. Nomination & Selection.

A5.3.1. Nominations will be made to HQ AFMC/SCPI. They can ve sent via e-mail or submitted via web entry and must contain the URL of the site nominated, and specify whether it is public or restricted access. This is designed as a "team concept" award; administrators, workgroup managers, and page maintainers should work as a team preparing a site for competition using AFI 33-129, command guidance and general "user-friendly" criteria. This refers to no "dead links," ease of navigation, effective use of graphics, etc. Any site not in compliance with web site security policy cannot be considered for recognition.

A5.3.2. Selection boards will consist of not less than 3 members (2 or more from HQ AFMC and one from HQ AFMC/PA). Evaluation will be done on a formatted score sheet using a categorical system. Points will be awarded based on the evaluation of board members with different categories assigned point values. All board members will review the web site and score it based on the assigned point value. Cumulative scores will be used to determine the best site. Any site not in compliance with web site security policy cannot be considered for recognition.

A5.3.3. Nominations will contain the following information:

A5.3.3.1. Exact URL of the nominated site.

A5.3.3.2. Organizational Level of Site (Center/Wing, Group/Squadron, etc)

A5.3.3.3. Domain of site (Public Access or restricted).

A5.3.3.4. Name of organization commander and web-server administrator/page maintainers

A5.4. Recognition. HQ AFMC Director of Communications and Information will approve all winners and will have final review authority over all scoring.   Once a winning site is selected, its owning commander will receive a congratulatory letter from HQ AFMC/SC and a certificate of achievement, and may post the recognition (via banner) to their site if desired.

A5.5. Timeframe of Award. Awards will be held on a quarterly basis, along with an annual competition. We hope in preparing for competition site maintainers conduct their reviews and submit their "best."

A5.6. Goal. We hope to improve our command web-site processes and recognize those who have gone the "extra e-mile" in making their sites functional, informational, and user-friendly while exceeding compliance with standards. Any site not in compliance with web site security policy cannot be considered for recognition.

Debra Haley, SES, Director
Communications and Information